一个可追踪密钥的策略隐藏属性基加密方案 *

欧毓毅，刘春龙

(广东工业大学 计算机学院，广州 510006)

摘　要：传统的属性基加密方案中存在着访问策略所包含的属性会泄露用户的敏感信息以及恶意用户泄露私钥获取非法利益而不会被追责的问题。同时私钥长度、密文长度和解密运算量均会随属性数量增加而带来较大的通信开销和计算开销。针对以上问题提出了一种可追踪且隐藏访问结构的属性基加密方案。该方案在不影响加/解密效率的前提下提高了加密算法的安全性，并采用双因子身份认证机制实现了更安全高效的访问控制。并且引入一个安全的签名机制用于支持可追踪密钥来追踪恶意用户。该方案基于 DBDH 假设，在标准模型下被证明是安全的。

关键词：基于属性加密；可追踪；隐藏策略；双因子身份验证

中图分类号：TP391　　doi: 10.3969/j.issn.1001-3695.2018.05.0316

Policy-hidden attribute-based encryption scheme with traceabe keys

Ou Yuyi, Liu Chunlong,

(*School of Computers Guangdong University of Technology*, *Guangzhou* 510006, *China*)

Abstract: In the traditional attribute-based encryption scheme, there are problems that the attributes contained in the access policy may leak sensitive information of the user and the malicious user leaks the private key to gain illegal profits without being blamed. At the same time, with the increase of the number of attributes the length of the private key, ciphertext, and the decryption operation will increase and it bring greater communication overhead and computational overhead. To solve these problems, an attribute-based encryption scheme that can track keys and hide the access structure is proposed. The scheme improves the security of the encryption algorithm without affecting the efficiency of encryption and decryption. The scheme adopts a two-factor authentication mechanism to achieve more secure and efficient access control, and it use a secure signature mechanism for supporting traceable keys to track malicious users. Finally, the theoretical analysis show that our scheme proved to be safe under the standard model based on the DBDH hypothesis.

Key words: attribute-based encryption; traceability; hidden policies; two-factor authentication

0　引言

云存储以分布式计算技术为基础，在开放的网络环境下为用户提供了强大的共享和存储能力，然而传统的加密技术已经不能满足用户对于细粒度的访问控制要求[1]。因此，为了实现加密数据的细粒度访问控制，Sahai 等人[1]于 2005 年首先提出的一种新的公钥加密机制——属性基加密（ABE），实现了公钥密码体制一对多的加密。为了表示更灵活的访问控制策略，相关学者在之后又提出了密钥策略属性基加密[2]和密文策略属性基加密[2]两类 ABE 加密机制。在对于密文策略的属性加密方案，加密者使用访问结构加密消息，解密者根据自身所拥有的属性预先从一个可信的授权方获取解密密钥，如果解密者本身的属性不满足嵌入在密文中的访问结构，解密者将不能解密该密文。

然而在传统的密文策略属性基加密方案中，访问策略和加密的明文往往会被一起发送给解密者，而访问结构有可能包含着与明文相关的信息，一旦密文被截获，加密者的隐私将有被泄露的风险。为了解决该问题，出现了许多隐藏访问结构的密文策略属性基加密方案。2007 年，Kapadia 等人[3]通过引入一个可信第三方，首次提出可匿名的密文—策略属性基加密方案，但该方案不能抵抗合谋攻击。之后，文献［4，5］分别以不同的形式实现了策略半隐藏，但文献［5］没有实现密钥追踪。文献［3，6～8］均实现了策略完全隐藏，但是均没有实现密钥追踪，即无法对恶意泄露信息的用户进行追踪。随后，文献［9］提出一个高表达力并可对恶意用户进行白盒追踪的 CP-ABE 方案，可以对恶意用户进行追踪，但性能开销较大。文献［10］提出支持大规模属性空间的可追踪方案。但文献［9,10］均不对访问策略进行隐藏。文献［5］提出了一个可追踪并隐藏部分属性的密钥策略基于属性加密方案，该方案将属性集分为公共正常属性集、隐藏正常属性集、隐藏身份相关属性集三个子集，

收稿日期：2018-05-21；修回日期：2018-07-02　　基金项目：广东省教育部产学研合作资助项目（2014B090901053）

作者简介：欧毓毅（1974-），女，副教授，主要研究方向为计算机网络系统集成；刘春龙（1994-），男，江西赣州人，硕士研究生，主要研究方向为信息安全（740605060@qq.com）.

但方案只能隐藏部分属性，且密文和用户公钥长度较长。在实际应用中，过长的密文会带来较大的通信开销。文献[11]同时实现了可追踪和策略完全隐藏，但是该方案的公钥长度有所增加。

在云存储环境下，基于属性加密（ABE）的加密方案可以实现灵活的用户访问控制，其中身份认证是访问控制的第一道防线，是云存储环境安全的基础。双因子身份认证是一种强化的网络访问控制机制，它为登录过程增加了额外的安全层。因此采用文献[8]中的双因子身份验证机制,实现更安全高效的访问控制。并且由于基于属性加密的特点，用户私钥只与一组描述用户的属性相关，在实际应用中，合法用户可能会为了获取利益，恶意地将私钥泄露给非法用户而无法被追究责任。因此增加身份认证的过程以及设计能对泄露信息的用户进行追踪的加密方案具有现实意义。

本文在文献[7]的系统模型上，结合文献[11]的签名机制和文献[8]中的双因子身份验证机制提出一种具有可追踪性并隐藏访问结构的属性基加密方案。首先利用双因子身份验证机制初步判断用户的合法性；然后利用访问树将访问结构嵌入密文中，多值与门转换为访问树来表达访问结构，访问结构中的每个属性可以取多个值，增加了系统的灵活性，通过降低双线性对的运算数量提高了加密和解密的效率。方案基于判断性 DBDH 假设，在标准模型下被证明是安全的。

1 相关工作

1.1 双线性映射

设群 G_1、G_2 和 G_T 均是阶为素数 p 的乘法循环群，g、h 分别是是群 G_1、G_2 生成元，一个映射 e: $G_1 \times G_2 \rightarrow G_T$ 是非对称双线性映射，若映射 e 满足下列特征：

a）双线性。对于 $\forall a$、$b \in Z_p$，都有等式 $e(g^a,h^b)=e(g,h)^{ab}$

b）非退化性。$e(g,h) \neq 1$

c）可计算性。对于任意的 g、h，能够在有效的多项式时间算法内计算 $e(g,h)$

1.2 访问结构

在本文中，用户的身份由特定的属性集合来表示，访问结构使用多值与门来表达。令 $U=\{att_1,att_2,\ldots,att_N\}$ 代表一个所有可能的属性取值集合，系统中属性个数为 n，ni 表示第 i 个属性的取值个数 $S_i = \{att_{i,1},att_{i,2},\ldots,att_{i,ni}\}$ 是一个属性可能的取值集合，其 ni 为属性 S_i 可能取值的个数。用户的属性列表为 $L=[L_1,L_2,\ldots,L_n]$，其中 $L_i=att_{i,t},t \in (1,2,\ldots,ni)$。访问结构为 $W=[W_1,W_2,\ldots,W_n]$，其中 $W_i \subset S_i$。对于 $\forall i=1,2,\ldots,n$，若 $L_i \in W_i$，则称用户属性列表 L 满足访问结构 W。

本文方案中用多值与门来表达访问结构，以增加系统的灵活性。在加密消息之前，加密者首先将访问结构转换成一棵访问树 τ，访问树的中间节点表示 ∧、∨ 运算符，叶子节点表示属性。密文中不能显示地包含访问树，访问时由加密者隐式地嵌入到密文中，因此，解密者仅仅知道他自己是否有能力解密该密文，而不能获得任何有关其他能够解密该密文的解密者信息。图 1 给出了由访问结构 $W=\left[\{att_{1,1},att_{1,2}\},\{att_{2,2}\},\{att_{3,1},att_{3,2},att_{3,3}\},\{att_{4,3}\}\right]$ 转换而成的访问树 τ。有很多属性集合可以满足图 1 中的访问树，如属性集 $S=\{att_{1,1},att_{2,2},att_{3,3},att_{4,3}\}$ 以及 $S=\{att_{1,2},att_{2,2},att_{3,1},att_{4,3}\}$ 等，但是如属性集 $S=\{att_{2,2},att_{3,2},att_{4,3}\}$ 以及 $S=\{att_{1,1},att_{2,2},att_{3,3}\}$ 等是不满足图 1 中的访问树的。

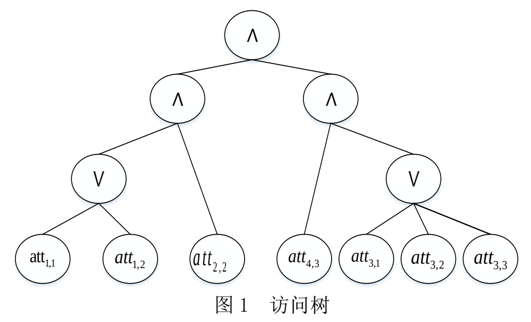


图 1 访问树

1.3 安全模型

对于用户口令认证协议攻击者模型一直沿用经典的 Dolev-Yao 模型[18]，即攻击者可任意侦听、截获、插入、删除或阻断流经公开信道中的消息。近年来，随着边信道攻击技术的发展（如功耗攻击、电磁场攻击和时间攻击），攻击者 A 可分析出智能卡内安全参数，攻击能力得到增强。本文攻击者能力如表 1 所示。

表 1 攻击者拥有的能力

能力	含义
C-00	A 可以离线穷举 $\lvert D_{id}\rvert \times \lvert D_{pw}\rvert$ 中所有元素。
C-01	A（非评估隐私安全）可以获取用户身份标识 ID。
C-1	A 任意侦听、截获、插入、删除或阻断流经公开信道中的消息，对于双因子协议，A 可以（1）获取用户口令；（2）提取智能卡内秘密信息，但二者不可兼得，否则为平凡攻击。
C-2	A 可以获取过期的会话密钥。
C-3	A 可以获知服务器长期私钥，此能力仅用于评估系统终极失效时的强健性。

本文方案可在选择属性模式下达到选择明文攻击的密文不可区分性，其所基于的安全模型[19]通过以下攻击者 A 与挑战者 B 之间的交互游戏进行描述。

初始化阶段：A 提供给 B 两个挑战访问结构 W_0 和 W_1。挑战者 B 选定安全参数 λ 并运行初始化算法得到公钥 PK 和主密钥 MSK。B 将 PK 发送给 A，并保留主密钥 MSK。

第一阶段：攻击者 A 提供一个属性列表 L，属性列表 L 不满足访问结构 W_0 和访问结构 W_1 是挑战访问结构的要求。满足要求时挑战者 B 才运行私钥产生算法，并将私钥 SK 发送给攻击者 A。攻击者可以进行多项式次数的询问。

挑战阶段：攻击者 A 提交 2 个长度相等的消息 M_0 和 M_1 给挑战者 B。挑战者 B 随机选取一个 M_b^*，用 W_b^*进行加密。挑战者运行加密算法并将密文返回给攻击者。

第二阶段：重复第一阶段和挑战阶段的过程，继续私钥询问。

猜测阶段：如果 $T = e(g,g)^{abc}$，则表明攻击者 A 就能准确

输出对 b 的猜测 b*；否则，$T = e(g,g)^z$，攻击者 A 只能做一个随机的猜测。如果 b*=b，B 输出 $\beta=1$；否则，输出 $\beta=0$。

攻击者获得攻击游戏胜利的优势定义为 $Adv(A)=\left|\Pr\left[b^*=b\right]-\frac{1}{2}\right|$。

定义 1 在多项式时间内，若不存在以不可忽略的优势赢得上述游戏的多项式时间攻击者，则称该隐藏访问结构的密文策略基于属性加密方案是选中明文安全的。

1.4 方案定义

方案由用户注册（Registration）、身份验证（Verification）、初始化算法(Setup) 、密钥生成算法(Keygen) 、加密算法(Encrypt) 、解密算法(Decrypt) 和追踪算法(Trace) 等算法组成。方案中采用双因子身份验证机制，每个用户有其唯一 ID 和登录密码 PW。解密时先进行用户登录，根据验证体制对用户身份进行第一道的判断，提高了攻击者破解合法用户身份信息伪装成合法授权用户的难度。通过身份验证后，用户分别将自己具有的属性私钥分量分别代入进行解密计算，验证用户私钥是否满足访问结构。若满足访问结构，则解密密文。下面分别对各种算法进行描述:

Registration 注册用户，用户输入身份 ID 和密码 PW，授权机构选取系统参数 c、b 以及当前注册时间 t 进行计算得到 $\{M,N,y\}$ 返回给用户。

Verification 身份验证,用户登录输入身份 ID 和密码 PW，根据验证算法，对用户身份进行第一道的判断，验证用户身份信息是否合法。

Setup 初始化算法，由授权机构完成。系统建立输入安全参数 λ，输出主密钥 MSK 和公共参数 PK。并产生一个包含二元组(k，ID) 的查询列表 T，初始化时查询列表 T 为空集。

Keygen 密钥生成算法，输入主密钥 MSK、属性列表 L、公钥 PK 和用户身份 ID，输出关于属性列表 L 的私钥 SK。并将二元组(k，ID)存入查询列表 T 中。

Encrypt 数据加密算法，由信息发送方完成。输入需要加密的明文消息 M，访问策略 W 和公共参数 PK，并输出密文 CT 。

Decrypt 加密算法，信息接收者输入公钥 *PK* 、隐式地嵌入访问结构 *W* 的密文 *CT* 和包含属性列表 *L* 的用户私钥 *SK* 。当解密密钥中的属性满足密文中的访问结构时，可以正确解密，得到信息 M，否则输出⊥。

Trace 追踪算法，输入用户的公钥 *PK* 、私钥 *SK* 和查询列表 T。先验证私钥 *SK* 是否标准定义的，若验证成功，输出与 *SK* 对应的用户身份 ID，否则输出符号⊥。定义符号⊥表示该用户私钥不用追踪。

2 方案构造

本文在文献[7]的系统模型上，采用双因子身份认证体制，提出了一种可追踪且隐藏访问结构的 CP-ABE 加密方案。

2.1 用户注册

Registration（ID，PW）

双因子身份验证的实施需要两个阶段来完成，即注册阶段和验证阶段。为了方便描述给出如下定义：S 为远程服务器，U 为用户，哈希函数 $H_i=\{0,1\}^*=\{0,1\}^{li}$，$i=1,2,3$。权威机构 S 的私钥为 x，计算 $y=g^x mod\ p$，用户输入身份 ID 和密码 PW，客户端 SC 选取随机数 c。计算 $H_0(c\|PW)$，将 $\{ID,H_0(c\|PW)\}$ 发送给权威机构 S，S 选取随机数 b，根据用户注册时间 t 进行计算：$M=H_0(H_0(ID)\oplus H_0(c\|PW))$，$N=H_0(c\|PW)\oplus H_0(x\|ID\|t)$，并将 $\{ID,t,c\}$ 存储在用户数据库中，$\{M,N,y\}$ 保存在智能卡 SC 中。

2.2 身份验证

Verification（ID，PW）

用户登录输入身份 ID*和密码 PW*，智能卡 SC 执行下列操作：

计算 $M^*=H_0(H_0(ID^*)\oplus H_0(c\|PW^*))$，若 $M^*=M$，SC 选取随机数 d，计算：

$Y_1=g^d mod\ p$，

$Y_2=y^d mod\ p$，$K=H_0(x\|ID\|t)=N\oplus H_0(c\|PW)$，$CID=ID^*\oplus H_0(Y_1\|Y_2)$，$CMK=(b\|K)\oplus H_0(Y_1\|Y_2)$，$M_2=\{H_0(Y_2\|K\|CID\|CMK)\}$。

用户将 $\{Y_2,CID,CMK,M_2\}$ 发送给权威机构 S。

根据用户登录请求信息，S 执行以下操作：计算 $M_2^*=\{H_0(Y_1\|K\|CID\|CMK)\}$，验证 $M_2^*=M_2$ 是否成立，若成立，则计算 $C_2=H_1(ID\|Y_2\|C_1\|K\|K_s)$ 并将 C_2 发送给 U。

接收到来自权威机构 S 的消息后，SC 执行计算：$C_2^*=H_1(ID\|Y_2\|Y_1\|C_1\|K\|K_u)$，验证 $C_2^*=C_2$ 是否成立。若成立计算：$C_3^*=H_2(ID\|Y_2\|Y_1\|C_1\|K\|K_s)$，用户将 C_3 发送给权威机构 S。

S 接受后执行以下操作：计算 $C_3^*=H_2(ID\|Y_2\|Y_1\|C_1\|K\|K_s)$ 验证 $C_3^*=C_3$ 是否成立，若成立，则验证通过，则开始执行加密算法，若不通过则返回⊥。

2.3 加密算法

令 $U=\{att_1,att_2,\ldots,att_N\}$ 代表一个所有可能的属性取值集合，$S_i=\{att_{i,1},att_{i,2},\ldots,att_{i,ni}\}$ 是一个属性可能的取值集合，其 *ni* 为属性 S_i 可能取值的个数。用户的属性列表为 $L=[L_1,L_2,\ldots,L_n]$，其中 $L_i=att_{i,t},t\in(1,2,\ldots,ni)$。访问结构为 $W=[W_1,W_2,\ldots,W_n]$，其中 $W_i\subset S_i$。

1） $Setup(1^\lambda)$

初始化算法输入安全参数 λ，定义一个双线性映射 $e: G_1\times G_2\to G_T$，G_1 和 G_2 是阶为素数 p 的乘法循环群，g_1、g_2 分别是是群 G_1、G_2 生成元，随机选取 $y\in Z^*_p$，$a_{i,j}\in Z^*_p$，并计算 $Y=e(g_1,g_2)^y$ 和 $A_{i,j}=g_1^{a_{i,j}}$。

输出：公钥 $PK=\left(e,g_1,g_2,Y,A_{i,j}\right)$ 和主密钥 $MSK=\left(y,a_{i,j}\right)$，其中 $i\in[1,n],j\in[1,n_i]$。同时生成一个包含二元组的(k，ID)的查询列表 T，初始化时列表为空集 ф。

2）$Keygen(PK,MSK,ID,L)$

输入：系统公钥 PK、系统主私钥 MSK 以及用户的属性列表 $L=[L_1,L_2,L_3,\ldots,L_n]$。对于 $1\le i\le n$，授权中心 CA 选择 $r\in Z^*_p$，计算 $k=r$，$D_0=g_2^{(y-r)/k}$，$D_{i,j}=g_2^{\,r}A_{i,j}^{-1}$

输出：用户私钥 $SK=\left(k,D_0,\{D_{i,j}\}_{\{i\in[1,n],j\in[1,ni]\}}\right)$。同时将二元组 (k,ID) 存入查询列表 T。

3）$Encrypt(PK,W,M)$

输入：系统公钥 PK、明文 M、相关的访问结构 $W=[W_1,W_2,\ldots,W_n]$。加密者首先将使用多值与门表达的访问结构按转换规则转换成对应的访问树 τ。加密者选择 $s\in Z^*_p$，后按规则为访问树的每一个孩子节点 i 选择 $s_i\in Z^*_p$，其中 $s=\sum_{i=1}^{N}s_i$。计算 $C_0=g_1^{\,s}$，$C_1=M\cdot e(g_1,g_2)^{ys}$，$C_{i,j}=A_{i,j}^{\,si}$

输出：密文 $CT=\left(C_0,C_1,\{C_{i,j}\}_{\{i\in[1,n],j\in[1,ni]\}}\right)$

2.4 解密算法

$Decrypt(PK,CT,SK)$

输入：系统公钥 PK、隐式地嵌入访问结构 W 的密文 CT 和包含属性列表 L 的用户私钥 SK。计算

$$M=\frac{C_1}{e(C_0^{\,k},D_0)\prod_{1}^{n}e(C_{i,j},D_{i,j})}$$

输出：明文 M。

2.5 追踪算法

$Trace(PK,T,SK)$

追踪算法可以分为验证和查询两个阶段。根据输入的用户公钥 PK、私钥 SK 和查询列表 T，输出用户 ID 或符号⊥。

1）验证阶段　在验证阶段，根据如下几个公式验证私钥 SK 是否合法，即符合标准形式下的密钥。验证方法如下：

$k\in Z^*_p,\ D_0,D_{i,j}\in G_2$

$$e(g_1,D_0)=e(g_1,g_2^{(y-k)/k})\ne 1$$

$$e(g_1,D_{i,j})=e(g_1^{\Sigma-aij},g_2^{-k})$$

2）查询阶段　若验证私钥 SK 是有效的用户私钥，则根据查询列表 T 中查询 k，并输出与 k 对应的用户 ID。若验证无效，则输出符号⊥。

3　方案分析

3.1 安全性分析

3.1.1 双因子认证安全分析

针对表 1 中攻击者 A 的 C-00 能力，方案中采用了公钥技术，由于不能得到用户的属性私钥，即使通过离线穷举得到正确用户的 ID 和 PW，同样不能访问加密文件。针对表 1 中 C-01 能力，即用户匿名性的基本要求：对用户 ID 进行 Hash 运算进行保护，攻击者不能获取用户的身份标志 ID。针对表 1 中 C-1 能力，即用户匿名性的高层次要求：采用了两次 Diffie-Hellan 密钥交换技术和公钥密码技术结合方式，攻击者即使能够得到智能卡中的参数和公钥，没有私钥仍然也不能破解其他人的不可追踪性。现有研究已经从理论上证明，要实现多因子安全性，采用公钥技术是实现用户匿名性、抗离线口令猜测攻击、前向安全性的必要条件[20]。针对表 1 中 C-3 能力，即用户前向安全性问题：引入传统的 Diffie-Hellman 密钥交换技术，每次验证都使用不同临时值 g^x 和 g^y，不能根据过期的会话密钥破解下一次的密钥。

3.1.2 抵抗选择明文攻击

定理 1　如果一个概率多项式时间内的攻击者 A 没有不可忽略的优势赢得选择性明文攻击下的安全游戏，则该方案是安全的。

证明　若攻击者 A 能以不可忽略的优势 $\varepsilon/2$ 来攻破本文方案，那么存在一个挑战者 B 能以相同的优势 $\varepsilon/2$ 来打破 $DBDH$ 假设。具体过程描述如下：

挑战者给定挑战元组 $[g,g^a,g^b,g^c,Z]$，其中 Z 的取值与 $e(g,g)^{abc}$ 在 G_T 中具有相同的概率分布。

初始化阶段：A 提供给 B 两个挑战访问结构 $W_0=[W_{0,1},W_{0,2},\ldots,W_{0,n}]$，$W_1=[W_{1,1},W_{1,2},\ldots,W_{1,n}]$，B 抛币得到随机值 $b\in\{0,1\}$。B 令 $Y=e(g^a,g^b)=e(g,g)^{ab}$，即有 $y=ab$。对于 $1\le i\le n,1\le j\le ni$，随机选取 $a_{i,j}\in Z^*_p$，当 $att_{i,j}\in W_{b,i}$ 时，算法 B 令 $A_{i,j}=g_1^{\,ai,j}$，当 $att_{i,j}\notin W_{b,i}$ 时，令 $A_{i,j}=g_1^{\,ai,jb}$。挑战者 B 把系统公钥 $PK=(e,g_1,g_2,Y,A_{i,j})$ 发送给攻击者 A，挑战者 B 自己保留主密钥 MK。

第一阶段：攻击者 A 提供一个属性列表 $L=[L_1,L_2,L_3,\ldots,L_n]$，属性列表 L 不满足访问结构 W_0 和访问结构 W_1 是挑战访问结构的要求，所以一定存在一个 $j\in[1,n]$，使得 $L_j\not\subseteq W_{b,j}$。挑战者 B 选择 $r\in Z^*_p$，计算 $k=r$，$D_0=g_2^{(y-r)/k}$，$D_{i,j}=g_2^{\,r}A_{i,j}^{-1}$，挑战者 B 将私钥 $SK=\left(k,D_0,D_{i,j\{i\in[1,n],j\in[1,ni]\}}\right)$ 发送给攻击者 A。

第二阶段：攻击者 A 提交 2 个长度相等的消息 M_0 和 M_1 给挑战者 B，挑战者 B 随机 $s_i\in Z^*_p$，其中 $s=\sum_{i=1}^{N}s_i$，计算 $C_0=g_1^{\,s}$，如果 $i=j$，则 $C_1=M_b^{\,*}\cdot e(g_1,g_2)^{ys}$，$C_{i,j}=A_{i,j}^{\,si}$；如果 $i\ne j$，则 $C_1=M_b^{\,*}\cdot e(g_1,g_2)^{z}$，$C_{i,j}=A_{i,j}^{\,si}$。

第三阶段：重复第一阶段和第二阶段的过程，继续私钥询

问。

猜测阶段：如果 T $=e(g,g)^{abc}$，则表明攻击者 A 就能准确输出对 b 的猜测 b^*；否则，T $=e(g,g)^{z}$，攻击者 A 只能做一个随机的猜测。如果 $b^*=b$，B 输出 $\beta=1$；否则，输出 $\beta=0$。

因此，挑战者 B 能够以 $\varepsilon/2$ 的优势解决 $DBDH$ 问题，即在 $DBDH$ 假设下，证明提出的方案是安全的。

3.1.3 抵抗用户窜谋攻击

本方案采用双因子身份验证机制，每个用户有其唯一 ID 和登录密码 PW。用户进行数据加密上传和获取解密文件前先进行用户登录，根据验证体制对用户身份进行第一道的判断，提高了攻击者破解合法用户身份信息伪装成合法授权用户的难度。通过身份验证后，用户分别将自己具有的属性私钥分量分别代入进行解密计算，验证用户私钥是否满足访问结构。该方案中用户只能知道自己是否具有访问秘密文件的条件，但不能获知自己能够满足访问结构的具体属性表达式，这就有效防止了多个非法用户或腐化用户窜谋，结合属性私钥获取解密密钥，获取共享文件，或者低授权用户进行越权盗取高级加密文件的风险。

3.1.4 白盒可追踪性

数据拥有者的数据在上传至云服务器之前首先进行身份认证，认证成功后使用访问策略 W 加密，只有授权的用户才能在解密服务器的帮助下解密出明文。

用户解密之前也需要进行身份认证，并且用户私钥生成时中加入因子 k，同时，将二元组 (k,ID) 存入查询列表 T。为了能解密得到密文，攻击者必须具备系统公钥 PK、密文 CT 和私钥 SK，并且属性集合必须满足访问控制策略。数据提供者可以根据用户的私钥 SK、系统公钥 PK，首先验证私钥 SK 是否标准定义的，若验证成功，根据因子 k 查询列表 T 后输出与 SK 对应的用户身份 ID，否则输出符号⊥。

3.2 效率分析

属性基加密机制的效率问题主要考虑通信开销和计算开销。一方面密文长度决定了通信开销，降低密文长度可以减少通信开销；另一方面 ABE 一对多的通信方式，使得系统中解密相对加密是一个高频行为，且双线性对的计算效率要低于其他运算，减少解密过程中双线性对的计算次数，可以有效降低计算开销。因此本文现将本文方案与所列文献中的方案分别从加/解密时间开销、功能特征和密文长度、私钥长度等相关参数方面进行比较。其中系统中属性个数为 n，ni 表示第 i 个属性的取值个数，$N=\sum_{i=1}^{n} ni$ 表示属性空间中所有属性的取值总个数，$|G|$、$|G_T|$ 和 $|Z_P^*|$ 表示 G、G_T 和 Z_p^* 中元素的单位长度，G、G_T 分别为群 G、G_T 上计算所用的时间，C_ε 表示双线性对所需要的时间。具体比较结果如表 2～4 所示。

表 2　方案功能特征比较

方案	可追踪性	策略隐藏	双因子认证
文献[4]	无	部分隐藏	无
文献[5]	可追踪	部分隐藏	无
文献[6]	无	完全隐藏	无
文献[7]	无	完全隐藏	无
文献[8]	无	完全隐藏	有
文献[9]	可追踪	无	无
文献[10]	可追踪	无	无
文献[11]	可追踪	完全隐藏	无
本文方案	可追踪	完全隐藏	有

表 3　方案的相关参数大小

方案	PK	MK	SK	CT
文献[11]	$(N+3)\|G\|+\|G_T\|$	$(N+2)\|Z_P^*\|$	$(n+1)\|G\|$	$(2n+1)\|G\|+\|G_T\|$
文献[7]	$(N+1)\|G\|+\|G_T\|$	$N\|Z_P^*\|+\|G_T\|$	$(2n+1)\|G\|$	$(2n+1)\|G\|+\|G_T\|$
本文方案	$(N+1)\|G\|+\|G_T\|$	$N\|Z_P^*\|+\|G_T\|$	$(n+1)\|G\|$	$(n+1)\|G\|+\|G_T\|$

表 4　时间开销

方案	加密时间	解密时间
文献[11]	$(n+1)G+G_T$	$(2n+1)C_\varepsilon+3G_T$
文献[7]	$(2n+1)G+G_T$	$(2n+1)C_\varepsilon+3G_T$
本文方案	$(n+1)G+G_T$	$(n+1)C_\varepsilon+3G_T$

从表 2 可以看出，文献[4～8]只实现了策略隐藏，文献[9，10]只实现了密钥可追踪。文献[5]虽然同时实现了可追踪和策略隐藏，但只能对策略部分隐藏。文献[11]也同时实现了可追踪和策略完全隐藏，但是该方案的公钥长度有所增加，本文方案可以同时实现可追踪和策略隐藏，并使用双因子身份验证机制，可以有效的抵抗用户合谋攻击。

如表 3 所示，本文方案虽然与文献[7]的系统公钥长度和主密钥长度一样，但是比文献[11]的短，其用户私钥长度与文献[7]一样,比文献[11]的短，加密所得到的密文长度比文献[11，7]的都短，在数据访问人数比数据加密者多的情况下，私钥长度关系着授权中心的效率，而密文长度则关系着通信代价。

根据表 4 所示，本方案的加密时间文献[11]一样，但是解密时间均比文献[11]的更短，相比文献[7]来说加密时间和解密时间均更短，因为双线性运算代价减少了近一半，所以方案的效率得以提高。

4　结束语

本文提出了一个可追踪密钥且隐藏访问结构的密文策略属性基加密方案。在不影响加/解密效率的前提下，方案中结合双因子身份认证机制实现对用户身份的匿名认证，解决了用户敏感信息易被泄露、文件易被窃取的风险，并且证明了在 DBDH 假设下该方案能够抵抗选择明文攻击，实现了密文的不可区分

性。在保证数据安全性的同时，通过降低双线性对运算的数目，大大降低了通信开销和计算开销。但本方案的不足之处是只能进行白盒追踪，因此下一步工作是实现能够进行黑盒追踪的加密方案。

参考文献：

[1] Sahai A, Waters B. Fuzzy identity-based encryption [C]// Proc of International Conference on Theory and Applications of Cryptographic Techniques. [S. l.] : Springer-Verlag, 2005: 457-473.

[2] Goyal V, Pandey O, Sahai A, *et al.* Attribute-based encryption for fine-grained access control of encrypted data [C]// Proc of ACM Conference on Computer and Communications Security. [S. l.] : ACM Press, 2006: 89-98.

[3] Kapadia A, Tsang P P, Smith S W. Attribute-based publishing with hidden credentials and hidden policies [C]// Proc of Network and Distributed System Security Symposium. San Diego, California: [s. n.] , 2007: 179-192.

[4] 应作斌，马建峰，崔江涛. 支持动态策略更新的半策略隐藏属性加密方案 [J]. 通信学报, 2015, 36 (12): 178-189. (Ying Zuobin, Ma Jianfeng, Cui Jiangtao. Partially policy hidden CP-ABE supporting dynamic policy updating [J]. Journal on Communications, 2015, 36 (12): 178-189.)

[5] Yu Shucheng, Ren Kui, Lou Wenjing, *et al.* Defending against key abuse attacks in KP-ABE enabled broadcast systems [M]// Security and Privacy in Communication Networks. 2009: 311-329.

[6] 刘雪艳，郑等凤. 基于素数群完全隐藏访问结构的 CP-ABE 方案 [J]. 计算机工程, 2016, 42 (10): 140-145. (Liu Xueyan, Zheng Dengfeng. CP-ABE scheme based on prime group with fully hidden access structure [J]. Computer Engineering, 2016, 42 (10): 140-145.)

[7] 汪海萍，赵晶晶. 隐藏访问结构的密文策略的属性基加密方案 [J]. 计算机科学, 2016, 43 (2): 175-178. (Wang Haiping, Zhao Jingjing. Ciphertext-policy attribute-based encryption with anonymous access structure [J]. Computer Science, 2016, 43 (2): 175-178.)

[8] 沈学利，吕莹楠. 一种隐藏访问结构的文件层次属性加密研究 [J/OL]. 计算机应用研究, 2019, 36 (1): 1-2 [2018-05-17]. http://kns. cnki. net/kcms/detail/51. 1196. TP. 20180208. 1714. 084. html. (Shen Xueli, Lu Yingnan. Research on file hierarchy attribute encryption of hidden access structure [J/OL]. Application Research of Computers, 2019, 36 (1): 1-2 [2018-05-17]. http://kns. cnki. net/kcms/detail/51. 1196. TP. 20180208. 1714. 084. html.)

[9] Yadav U C. Ciphertext-policy attribute-based encryption with hiding access structure [C]// Advance Computing Conference. [S. l.] : IEEE Press, 2015: 6-10.

[10] Ning Jianting, Cao Zhenfu, Dong Xiaolei, *et al.* Large universe ciphertext-policy attribute-based encryption with white-box traceability [J]. 2014, 8713: 55-72.

[11] 王梅，孙磊. 一个安全可追踪的策略隐藏属性基加密方案 [J]. 计算机应用与软件, 2017 (2): 267-271. (Wang Mei, Sun Lei. A secure and traceable attribute-based encryption scheme with hiding access structure [J]. Computer Applications and Software, 2017 (2): 267-271)

[12] Ning Jianting, Cao Zhenfu, Dong Xiaolei, *et al.* White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes [J]. IEEE Trans on Information Forensics & Security, 2015, 10 (6): 1274-1288.

[13] Zhong Hong, Zhu Wenlong, Xu Yan, *et al.* Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage [J]. Soft Computing, 2016, 22 (1): 1-9.

[14] Odelu V, Das A K, Rao Y S, *et al.* Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment [J]. Computer Standards & Interfaces, 2017, 54 (P1): 3-9.

[15] Qin Baodong, Deng Robert H, Liu Shengli, *et al.* Attribute-based encryption with efficient verifiable outsourced decryption [J]. IEEE Trans on Information Forensics and Security, 2015, 10 (7): 1384-1393.

[16] Liu Zhen, Cao Zhenfu, Wong D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures [J]. IEEE Trans on Information Forensics & Security, 2013, 8 (1): 76-88.

[17] 陈露，王睛. 基于 ATP-ABE 的访问控制方案 [J/OL]. 计算机工程与应用, 1-9 [2018-05-17]. http://kns. cnki. net/kcms/detail/11. 2127. TP. 20180409. 1448. 016. html. (Chen Lu, Wang Wei. An access control scheme based on ATP-ABE [J/OL]. Computer Engineering and Applications, 1-9 [2018-05-17]. http://kns. cnki. net/kcms/detail/11. 2127. TP. 20180409. 1448. 016. html.)

[18] Dolev D, Yao A. On the security of public key protocols [J]. IEEE Trans on Information Theory, 1983, 29 (2): 198-208.

[19] Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures [M]// Applied cryptography and network security. Berlin: Springer, 2008: 111-129.

[20] 汪定，李文婷，王平. 对三个多服务器环境下匿名身份认证协议的安全性分析 [J/OL]. 软件学报, 1-16 [2018-06-25]. https://doi. org/10. 13328/j. cnki. jos. 005361. (Wang Ding, Li Wenting, Wang Ping. Crytanalysis of three anonymous authentication schemes for multi-server environment [J/OL]. Journal of Software, 1-16 [2018-06-25]. https://doi. org/10. 13328/j. cnki. jos. 005361.)